A Computer Motivated Study of
Problems in Number Theory

Mathematical Appendix

Michael Blinov[1], Nurit Zehavi[2] and Sarah Black[3]

[1] Mathematics Department, The Weizmann Institute of Science, Rehovot
e-mail: blinov@wisdom.weizmann.ac.il

[2] Science Teaching Deprtment, The Weizmann Institute of Science, Rehovot
e-mail: nurit.zehavi@weizmann.ac.il

[3] Mathematics Department, Michlala-Jerusalem College, Jerusalem, Israel
e-mail: sblack1@macam.ac.il

Note 1: Prime Number Theorem

The Prime Number Theorem. *The number of primes not exceeding N, $\pi(N)$ is asymptotic to $\dfrac{N}{\ln N}$.*

Legendre (1752-1833) and, after him, Gauss (1777-1855) conjectured that this number is approximately
$$\frac{n}{1 - \frac{1}{2} + \frac{1}{3} + \ldots \pm \frac{1}{n}}.$$

It was first proved in 1896 by Hadamard (1865-1963) and de la Vallée Poussin (1866-1962), and even today its proof is far from simple.

Note 2: Congruence modulo n

Definition. *Let n be a fixed positive number. Then a and b are said to be* **congruent modulo** *n, denoted by $a \equiv b \ (mod\,n)$, if $a - b$ is divisible by n, i.e. $a - b = kn$ for some $k \in \mathbb{Z}$.*

The congruence property is similar to the usual equality:

(1) $a \equiv a \ (mod\, n)$

(2) If $a \equiv b \ (mod\, n)$, then $b \equiv a \ (mod\, n)$.

(3) If $a \equiv b \ (mod\, n)$ and $b \equiv c \ (mod\, n)$, then $a \equiv c \ (mod\, n)$.

(4) If $a \equiv b \ (mod\, n)$ and $c \equiv d \ (mod\, n)$, then $a + c \equiv b + d \ (mod\, n)$ and $ac \equiv bd \ (mod\, n)$.

If we replace $\equiv \ (mod\, n)$ by $=$, we get the usual properties of integers $\mathbb{Z}$. Because of these properties, $\mathbb{Z}_n$, like $\mathbb{Z}$, is a ring.

Let us note, that any number $a \in \mathbb{Z}$ can be represented as $a = a_1 + kn$, where a_1 is among numbers $0, 1, \ldots, n - 1$. Therefore it is easy to see that the elements of $\mathbb{Z}_n$ are $0, 1, \ldots, n - 1$. We will return briefly to the notion of $\mathbb{Z}_n$ in note 6, but the essential point is that for any expression $f(x)$, the notation $f(x) \equiv 0 \ (mod\, n)$ means that $f(x)$ is divisible by n.

Note 3: Number representations and Chinese Remainder Theorem

(1) Any natural number can be uniquely written as $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, where p_i are distinct primes that divide n.

(2) If $f(x) \equiv 0 \ (mod\, p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s})$, where p_i are distinct prime numbers, then

$$\begin{cases} f(x) \equiv 0 \ (mod\, p_1^{k_1}) \\ \ldots\ldots\ldots\ldots \\ f(x) \equiv 0 \ (mod\, p_s^{k_s}). \end{cases}$$

For example, if an expression is divisible by 24, then it is divisible by 3 and 8.

(3) **"The Chinese Remainder Theorem"**: *Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, *where* p_i *are different primes. Then for any* $(a_1, a_2, \ldots, a_n)$ *there exists a unique* $x^* \in \mathbb{Z}_n$, *satisfying*
$x^* \equiv a_1 \ (mod\, p_1^{k_1})$,
$x^* \equiv a_2 \ (mod\, p_2^{k_2})$,
$\ldots\ldots\ldots\ldots\ldots$
$x^* \equiv a_s \ (mod\, p_s^{k_s})$.

Corollary 1: *Let* $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. *Assume that*
the congruence $f(x) \equiv 0 \ (mod\, p_1^{k_1})$ *has solutions* $(x_1^{(1)}, \ldots, x_{t_1}^{(1)})$,
the congruence $f(x) \equiv 0 \ (mod\, p_2^{k_2})$ *has solutions* $(x_1^{(2)}, \ldots, x_{t_2}^{(2)})$,
$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$
the congruence $f(x) \equiv 0 \ (mod\, p_s^{k_s})$ *has solutions* $(x_1^{(s)}, \ldots, x_{t_s}^{(s)})$.

Then for any set $(x_{i_1}^{(1)}, x_{i_2}^{(2)}, \ldots, x_{i_s}^{(s)})$, *there exists a unique* $x^* \in \{0, 1, \ldots, n - 1\}$, *which solves the equation* $x^2 - 1 \equiv 0 \ (mod\, n)$, *and for different sets these* x^* *values are different.*

Corollary 2: *Let $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Assume that
the congruence $f(x) \equiv 0 \ (mod \ p_1^{k_1})$ has T_1 solutions,
the congruence $f(x) \equiv 0 \ (mod \ p_2^{k_2})$ has T_2 solutions,*

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

*the congruence $f(x) \equiv 0 \ (mod \ p_s^{k_s})$ has T_s solutions.
Then $f(x) \equiv 0 \ (mod \ n)$ has $T_1 T_2 \cdots T_s$ solutions.*

Note 4: Formula for $F(n)$

Lemma 1. *The congruence $x^2 - 1 \equiv 0 \ (mod \ p^\alpha)$, where p is a prime number
greater than or equal to 3, has only two solutions $x = 1$ and $x = p^\alpha - 1$.*

Proof: $x^2 - 1$ divisible by p^α means that either $(x-1)(x+1) = 0$ or $(x-1)(x+1) = p^\alpha q$. In the first case we get the solution $x = 1$, in the second case we get

$$\begin{cases} x - 1 = p^\beta t \\ x + 1 = p^\gamma r, \end{cases}$$

where t, r are relatively prime to p and $\beta \geq 0$, $\gamma \geq 0$, $\beta + \gamma \geq \alpha$.

So, $x = p^\beta t + 1 = p^\gamma r - 1$, hence $p^\gamma r - p^\beta t = 2$. If $p \neq 2$, then the last equation does not have solutions if $\gamma > 0$ and $\beta > 0$ simultaneously, since then the right hand side of the equation is divisible by p, and the left hand side is not.

If $\beta = 0$, then $\gamma = \alpha + i$, where $i \geq 0$, so $x = p^\gamma r - 1 = p^\alpha p^i r - 1$ must be less than p^α and greater than or equal to 0, which is possible only for $i = 0$ and $r = 1$. Thus we obtain the solution $x = p^\alpha - 1$.

Similarly, if $\gamma = 0$, then $\beta = \alpha + i$, where $i \geq 0$, so $x = p^\beta t + 1 = p^\alpha p^i t + 1$ must be less than p^α, which is possible only for $t = 0$. This gives the solution $x = 1$.

Therefore, there are only two solutions in this case.

Lemma 2. *The congruence $x^2 - 1 \equiv 0 \ (mod \ 2^\alpha)$ has:*
   (1) one solution; $x = 1$ for $\alpha = 1$;
   (2) two solutions; $x = 1$ and $x = 3$ for $\alpha = 2$;
   (3) four solutions; $x = 1$, $x = 2^{\alpha-1} - 1$, $x = 2^{\alpha-1} + 1$, $x = 2^\alpha - 1$ for $\alpha \geq 3$.

Proof: The proof is similar to the proof of Lemma 1. Cases (1) and (2) are trivial. Consider case (3). $x^2 - 1$ is divisible by 2^α means that $(x - 1)(x + 1)$ is divisible by 2^α, which means that either $(x - 1)(x + 1) = 0$ or $(x - 1)(x + 1) = 2^\alpha q$. In the former we get the solution $x = 1$, in the latter we get

$$\begin{cases} x - 1 = 2^\beta t \\ x + 1 = 2^\gamma r, \end{cases}$$

where t, r are odd and $\beta \geq 0$, $\gamma \geq 0$ and $\beta + \gamma \geq \alpha$. We obtain $x = 2^\beta t + 1 = 2^\gamma r - 1$, hence $2^\gamma r - 2^\beta t = 2$.

The values β and γ cannot be equal to 0 simultaneously for then $\alpha = 0$ contrary to assumption. Neither one of them can be equal to 0, since an odd number on

3

the left hand side equals 2. Both of them cannot be greater than 1, since then the left hand side of the equation will be divisible by 4, and the right hand side – only by 2. So we are left with the possibility that precisely one of the numbers β, γ must be equal to 1.

If $\gamma = 1$, then $\beta \geq \alpha - 1$, so $\beta = \alpha + i - 1$, where $i \geq 0$.

$$x - 1 = 2^\beta t \quad \Rightarrow \quad x = 2^{\alpha+i-1}t + 1.$$

$$x < 2^\alpha \quad \Rightarrow \quad 2^{\alpha-1}(2^i t - 2) + 1 < 0 \quad \Rightarrow \quad t = 1,\ i = 0.$$

We get the solution $x = 2^{\alpha-1} - 1$.

If $\beta = 1$, then $\gamma \geq \alpha - 1$, therefore $\gamma = \alpha + i - 1$, where $i \geq 0$.

$$x + 1 = 2^\gamma r \quad \Rightarrow \quad x = 2^{\alpha+i-1}r - 1.$$

$$0 \leq x < 2^\alpha \quad \Rightarrow \quad 2^{\alpha-1}(2^i r - 2) - 1 < 0 \quad \Rightarrow \quad 2^i r - 2 \leq 0$$

We get either $r = 1$, $i = 0$, or $r = 1$, $i = 1$, which lead to the solutions $x = 2^{\alpha-1} - 1$ and $x = 2^\alpha - 1$, q.e.d.

Using corollary 2 of Note 3, we obtain the following:

Formula. *The number of solutions of the equation $x^2 - 1 \equiv 0 \ (mod\ n)$ is*
  1) 2^s, if $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, $p_i \geq 3$ $(1 \leq i \leq s)$ – distinct prime numbers;
  2) 2^s, if $n = 2p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, $p_i \geq 3$ $(1 \leq i \leq s)$ – distinct prime numbers;
  3) 2^{s+1}, if $n = 4p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, $p_i \geq 3$ $(1 \leq i \leq s)$ – distinct prime numbers;
  4) 2^{s+2}, if $n = 2^{k_0}p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, $p_i \geq 3$ $(1 \leq i \leq s)$ – distinct prime numbers,
$k_0 \geq 3$.

Note 5: Fermat's Little Theorem and Euler's Theorem

Fermat's Little Theorem. *If p is a prime number and a is an integer in $\mathbb{Z}_p$ (i.e. $a \in \{0, 1, \ldots, p - 1\}$), then*

$$a^{p-1} \equiv 1 \ (mod\ p),$$

i.e. $a^{p-1} - 1$ is divisible by p.

Euler's theorem. *If p is a prime number and a is an integer in $\mathbb{Z}_{p^\alpha}^*$ (i.e. $a \in \{0, 1, \ldots, p^\alpha - 1\}$ and $(p, a) = 1$), then*

$$a^{p^\alpha - p^{\alpha-1}} \equiv 1 \ (mod\ p^\alpha),$$

i.e. $a^{p^\alpha - p^{\alpha-1}} - 1$ is divisible by p^α.

Historically, Fermat's theorem was stated in 1640, and it was generalized by Euler in 1760. A special case of Fermat's theorem is that if p is a prime, then p

divides $2^p - 2$. The ancient Chinese knew this fact. Proofs of these theorems can be found in any number theory book.

Note 6: Primitive roots

In examples considered we saw that $\mathbb{Z}_n$ has multiplicative generators, i.e. elements $a \in \mathbb{Z}_n$ whose distinct powers yield $\mathbb{Z}_n^*$ (namely all $z \in \mathbb{Z}_n$ relatively prime to n). Thus, if p is a prime number, then $\mathbb{Z}_p^*$ consists of all elements of $\mathbb{Z}_p$ except 0.

Such numbers a, which generate the whole $\mathbb{Z}_n^*$, are called **primitive roots of** $\mathbb{Z}_n^*$. It follows that if a is a primitive root of $\mathbb{Z}_p^*$ for prime p, then the congruence $a^k \equiv 1 \ (mod \, p)$ has only two solutions $k = 0$ and $k = p - 1$. $\mathbb{Z}_p^*$ may have several primitive roots, for instance $\mathbb{Z}_5^*$ has both 2 and 3 as primitive roots, $\mathbb{Z}_7^*$ has 3 and 5 as primitive roots; note that, for example, 4 is not a primitive root of either of them.

One can show that for any prime $p \geq 3$ and for every natural number α there exists a primitive root of $\mathbb{Z}_{p^\alpha}^*$ (see, e.g. T. Nagell *"Number Theory"*, 1964 or N.H. McCoy *"The Theory of Numbers"*, 1965).

Note 7: Finding $F(n)$ using primitive roots theory for $n = p^\alpha$, $p \geq 3$

What is so valuable in our exploration of the notion of a primitive root? Assume that when we solve the congruence $x^2 - 1 \equiv 0 \ (mod \, p)$, p is an odd prime. If we know that a is a primitive root of $\mathbb{Z}_p$, then $x \equiv a^k \ (mod \, p)$ for some value of k. Then by Fermat's Little Theorem the congruence is $a^{2k} - 1 \equiv 0 \ (mod \, p)$. The number a is a primitive root, so this congruence has only two solutions $k = 0$ or $k = (p-1)/2$. Thus the case n is an odd prime is solved.

Now consider $n = p^\alpha$. If we are looking for solutions of the congruence $x^2 - 1 \equiv 0 \ (mod \, p^\alpha)$, then definitely they belong to the set $\mathbb{Z}_{p^\alpha}^*$ (since for $x = pk$, $x^2 - 1$ cannot be divided by any power of p). Similarly to the case for p, assume that a is a primitive root of $\mathbb{Z}_{p^\alpha}^*$, then $x \equiv a^k \ (mod \, p^\alpha)$ for some value of k. Thus, by Euler's Theorem the congruence is $a^{2k} - 1 \equiv 0 \ (mod \, p^\alpha)$. But since a is a primitive root, this equation has only the two solutions, $k = 0$ or $k = p^\alpha(p-1)/2$.

Note 8: Finding $F(n)$ using primitive roots theory for $n = 2^{\alpha}$

We can easily check that $\mathbb{Z}_2^*$ and $\mathbb{Z}_{2^2}^*$ both have primitive roots. However, $\mathbb{Z}_{2^n}^*$ for $n \geq 3$ does not have a primitive root (for if so the congruence would have two solutions, whereas it has 4 (see Lemma 2, note 4). Rather, $\mathbb{Z}_{2^n}^*$ has **two multiplicative generators**. For example, $\mathbb{Z}_{2^3}^* = \mathbb{Z}_8^*$ has generators 5 and 7, for $1 \equiv 5^2 \equiv 7^2 \,(mod\,8)$, $3 \equiv 5 \cdot 7 \,(mod\,8)$, $5 \equiv 5 \,(mod\,8)$, $7 \equiv 7 \,(mod\,8)$.

In the general case the multiplicative generators of $\mathbb{Z}_{2^n}^*$, $n \geq 3$ are 5 and $2^n - 1 \equiv -1 \,(mod\,2^n)$, and each of the elements of $\mathbb{Z}_{2^n}^*$ can be represented either as $x \equiv 5^k \,(mod\,2^n)$ for some value of k, or as $x \equiv (2^n - 1)5^k \equiv -5^k \,(mod\,2^n)$ for some value of k (See, e.g., Hua Loo Keng *"Introduction to Number Theory"* (Springer-Verlag, 1982) for proof that 5 and $2^n - 1 \equiv -1 \,(mod\,2^n)$ are multiplicative generators.)

One can show that the congruence $5^{2k} - 1 \equiv 0 \,(mod\,2^n)$ has two solutions $k = 0$ and $k = 2^{n-3}$, hence it gives us two solutions for the case $x \equiv 5^k$, namely $x = 1$ and $x = 2^{n-3} \equiv 1 + 2^{n-1} \,(mod\,2^n)$, and two solutions for the case $x \equiv -5^k$, namely $x = -1 \equiv 2^n - 1$ and $x = -2^{n-3} \equiv 2^{n-1} - 1 \,(mod\,2^n)$.

The congruences $2^{n-3} \equiv 1 + 2^{n-1} \,(mod\,2^n)$ and $2^n - 1$ and $x = -2^{n-3} \equiv 2^{n-1} - 1 \,(mod\,2^n)$ can be proved by induction. Such a proof can be found in Hua Loo Keng *"Introduction to Number Theory"*.

Note 9: Artin's conjecture

Let a be a fixed number, $\pi(N)$ be the number of primes less than or equal to N, $\nu_a(N)$ be the number of primes less than or equal to N for which a is a primitive root. What is the connection between these two numbers for different values of a and large values of N?

Artin's conjecture (1927): *If $a \neq b^n$ with $n > 1$, then $\nu_a(N) \sim A\,\pi(N)$, where A is Artin's constant, $A = 0.3739558....$*

But how could it be conceived at the beginning of the century, when fast computer calculations were fairy tales?

First of all, mathematicians are very hardworking, and such tables up to $N = 100\ 000$ were computed manually (!) in 1913 by Cunningham. The second point: different techniques are involved in Number Theory, and one of them has probability arguments. So, the following considerations made this conjecture plausible. We would like to outline the ingredients of its probabilistic proof. For complete proofs reader is referred to V. Klee, S. Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*.

Consider $a = 2$ and the primes $p \leq N$, where N is large enough. Let us count all p's less than N, s.t. 2 is a primitive root of $\mathbb{Z}_p^*$.

For every prime p choose any primitive root g_p of $\mathbb{Z}_p^*$. Then for some natural

m_p, $g_p^{m_p} \equiv 2 \, (mod\, p)$.

Claim 1. *2 is a primitive root of $\mathbb{Z}_p^*$ if and only if $(m_p, p - 1) = 1$.* (Outline of stages required for proof follows at the end.)

So, let $(m_p, p - 1) = G_p$. We have to find those p, for which $G_p = 1$. Let us eliminate from all primes less than N those p, for which $2|G_p$.

Claim 2. *Asymptotically, half of all primes p satisfy $2|G_p$.* (Outline of stages required for proof follows at the end.)

So we are left with $(1 - \frac{1}{2})\pi(N)$ primes for which 2 *can be* a primitive root, since 2 does not divide G_p.
   Next we eliminate those p for which $3|G_p$.

Claim 3. *There are $\frac{1}{3 \cdot 2}\pi(N)$ such primes among the all primes less than N.* (Outline of stages required for proof follows at the end.)

So we are left with $(1 - \frac{1}{2})(1 - \frac{1}{3 \cdot 2})\pi(N)$ primes for which 2 *can be* a primitive root, since 2 does not divide G_p and 3 does not divide G_p.
   Continuing eliminating primes p with $5 \mid G_p$, $7 \mid G_p$, etc., we are left with those p, for which $G_p = 1$, as no prime divides G_p. The number of such primes is $A\,\pi(N)$, where A (called Artin's constant) is given by $\prod\limits_{p} \left(1 - \dfrac{1}{p(p - 1)}\right)$. Exact computations (done in 1961 by J. W. Wrench, Jr.) gave A the following value:
$A = 0.37395\,58136\,19202\,28805\,47280\,54346\,41641\,51116.....$

   The cases of $a = 3, 5, 7, \ldots$ are considered similarly.

   Proof of claim 1 follows from the Fermat's Little theorem: $g^a \equiv 1 \, (mod\, p)$ if and only if $a \equiv 0 \, (mod\, p - 1)$.
   Proof of claim 2 follows from the following series of considerations, facts 1–3, difficulty of each of them is given in brackets – from trivial (*) to very difficult (***).

   Let us notice that $p - 1$ is always even, except for $p = 2$. So $(m, p - 1) = G_p$ is divisible by 2 if and only if m is odd.
   Fact 1.(*) *$m(g_p)$ is even for those p's, for which the equation $x^2 \equiv 2 \, (mod\, p)$ has a solution.*
   Fact 2.(**) *$x^2 \equiv 2 \, (mod\, p)$ is solvable for all primes $p = 4k + 1$ and unsolvable for all primes $p = 4k + 3$.*
   Fact 3.(***) *The number of primes of the form $p = 4k + 1$ is "asymptotically equal" to the number of primes of the form $p = 4k + 3$.*

   Proof of claim 3 follows from the series of similar considerations:

Fact 4.(***) *The number of primes of the form $p = 3k + 1$ is "asymptotically equal" to the number of primes of the form $p = 3k + 2$.*

Therefore $3|p - 1$ in one half of the cases.

Fact 5.(*) $3 \mid m(g_p)$ *in one-third of the cases.*

Fact 6.(*) *The events $3 \mid m(g_p)$ and $3 \mid G_p$ are independent.*